# The Trellis Complexity of Equivalent Binary [17, 9] Quadratic Residue Codes Is Five

*Yan-Yih Wang* *Chung-Chin Lu*
Department of Electrical Engineering
National Tsing Hua University
Hsinchu, Taiwan 300, R.O.C.

**Abstract:** It is known that equivalent linear block codes may have different minimal trellis structures. The minimum complexity among all minimal trellis structures of equivalent codes is defined as the trellis complexity of the class of equivalent codes. Sharper lower bounds for trellis complexity are derived when more information about the infrastructure of codes is supplied. These bounds serve as a starting specification for a search algorithm to find optimal permutations under which the permuted codes achieve the trellis complexity. A simple application to the class of equivalent binary [17, 9] quadratic residue codes finds the trellis complexity is five.

Let $\mathcal{C}$ be an $[n, k, d]$ linear block code over $GF(q)$. Let $\mathcal{D}$ be its dual code with minimum distance $d^\perp$. Let $S_n$ be the set of all permutations on the $n$ coordinates of codewords. Let $\sigma(\mathcal{C})$ be the equivalent code of $\mathcal{C}$ under a permutation $\sigma$ in $S_n$. Let $\sigma(\mathcal{C})_{p,i}$ ($\sigma(\mathcal{C})_{f,i}$) be the past (future) subcode of $\sigma(\mathcal{C})$ which consists of codewords whose future (past) coordinates to position $i$ are all zero. Let $k_{p,i}(\sigma)$ ($k_{f,i}(\sigma)$) be the dimension of the past (future) subcode $\sigma(\mathcal{C})_{p,i}$ ($\sigma(\mathcal{C})_{f,i}$). The dimension $k_{s,i}(\sigma)$ of the state space at position $i$ in a minimal trellis of $\sigma(\mathcal{C})$ is [1]

$$k_{s,i}(\sigma) = k - k_{p,i}(\sigma) - k_{f,i}(\sigma).$$

Let $s(\sigma(\mathcal{C}))$ be the maximum value of $k_{s,i}$ over $0 \le i \le n$. The trellis complexity $s$ of the class of equivalent codes of $\mathcal{C}$ is defined as

$$s = \min_{\sigma \in S_n} s(\sigma(\mathcal{C})).$$

Let

$$K_{p,i} = \max_{\sigma \in S_n} k_{p,i}(\sigma), K_{f,i} = \max_{\sigma \in S_n} k_{f,i}(\sigma), K_{s,i} = k - K_{p,i} - K_{f,i}.$$

Note that $K_{p,i} = K_{f,n-i}$. Since $k_{p,i}(\sigma) \le K_{p,i}$ and $k_{f,i}(\sigma) \le K_{f,i}$, we have

$$k_{s,i}(\sigma) \ge K_{s,i}.$$

In general, $K_{p,i}$ and $K_{f,i}$ are intrinsic attributes of the class of equivalent codes of code $\mathcal{C}$. $K_{f,i}$ may be estimated by $N(\alpha, \beta)$ [2] which is the minimum possible block length for a linear block code to have minimum distance $\alpha$ and dimension $\beta$ as follows:

1. If $i \le N(d^\perp, j) - 1$, then $K_{f,i} \le k - i + j - 1$.
2. If $i \ge n - N(d, j) + 1$, then $K_{f,i} \le j - 1$.

More precisely, for binary codes and early and late positions $i$, $K_{f,i}$ can be evaluated as follows:

$$K_{f,i} = \begin{cases} k - i, & \text{if } 0 \le i \le d^\perp - 1, \\ k - i + 1, & \text{if } d^\perp \le i < d^\perp + \left\lceil \frac{d^\perp}{2} \right\rceil - 1, \\ 1, & \text{if } n - \left(d + \left\lceil \frac{d}{2} \right\rceil - 1\right) \le i \le n - d, \\ 0, & \text{if } n - d + 1 \le i \le n. \end{cases}$$

Two monotone sequences $0 = \tilde{k}_{p,0} \le \tilde{k}_{p,1} \le \ldots \le \tilde{k}_{p,n} = k$ and $k = \tilde{k}_{f,0} \ge \tilde{k}_{f,1} \ge \ldots \ge \tilde{k}_{f,n} = 0$ together are called a specification of past and future dimensions if they satisfy

1. $0 \le \tilde{k}_{p,i} - \tilde{k}_{p,i-1}(\tilde{k}_{f,i-1} - \tilde{k}_{f,i}) \le 1, \forall 1 \le i \le n$;
2. $k - \tilde{k}_{p,i} - \tilde{k}_{f,i} \ge 0$ for all $0 \le i \le n$.

The minimal trellis structure of an equivalent code $\sigma(\mathcal{C})$ is said to be dominated by a specification as in above if all its past dimensions $k_{p,i}(\sigma)$ and future dimensions $k_{f,i}(\sigma)$ are upper bounded by $\tilde{k}_{p,i}$ and $\tilde{k}_{f,i}$ respectively at each position $i$. Necessary and sufficient conditions for the existence of a permutation $\sigma$ under which the minimal trellis structure of the permuted code is close to and dominated by a specification are developed. And a constructive algorithm is then built to search for optimal permutations under which permuted codes can achieve the trellis complexity.

Let $\mathcal{C}$ be the binary [17, 9] quadratic residue code generated by $g(x) = 1 + x^3 + x^4 + x^5 + x^8$.. Let $\mathcal{D}$ be its dual code, The minimum distance of $\mathcal{C}$ and $\mathcal{D}$ are $d = 5$ and $d^\perp = 6$. By applying the above results, we can list $K_{f,i}, K_{p,i}$, and $K_{s,i}$ in the following table:

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $K_{p,i}$ | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 2 | 2 | 3 | 4 | 4 | 5 | 6 | 7 | 8 | 9 |
| $K_{f,i}$ | 9 | 8 | 7 | 6 | 5 | 4 | 4 | 3 | 2 | 2 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| $K_{s,i}$ | 0 | 1 | 2 | 3 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 3 | 2 | 1 | 0 |

Hence, the trellis complexity of the class of equivalent binary [17,9] QR codes is not smaller than 5. To find optimal permutations and then to determine the exact trellis complexity, we start our search algorithm with the following specification of future and past dimensions $\tilde{k}_{p,i}$, $\tilde{k}_{f,i}$, a very slight variation from the above table, listed in the next table:

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\tilde{k}_{p,i}$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 2 | 3 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| $\tilde{k}_{f,i}$ | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 3 | 2 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| $\tilde{k}_{s,i}$ | 0 | 1 | 2 | 3 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 3 | 2 | 1 | 0 |

With the above specification, we have constructed four optimal permutations:

$$\begin{aligned} \sigma &= (1,4,5,6,9,7,10,2,14,17,3,15,8,11,12,13,16) \\ &\text{or } (1,4,5,6,9,10,7,2,14,17,3,15,8,11,12,13,16) \\ &\text{or } (1,4,5,6,9,7,10,2,14,17,15,3,8,11,12,13,16) \\ &\text{or } (1,4,5,6,9,10,7,2,14,17,15,3,8,11,12,13,16)\,. \end{aligned}$$

With anyone of the above permutations, we have

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $k_{p,i}(\sigma)$ | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 2 | 2 | 3 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| $k_{f,i}(\sigma)$ | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 3 | 2 | 2 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| $k_{s,i}(\sigma)$ | 0 | 1 | 2 | 3 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 3 | 2 | 1 | 0 |

Thus, the trellis complexity of the class of equivalent binary [17, 9] QR codes is 5.

[1] G. D. Forney, JR., "Coset codes – Part II: Binary lattices and related codes," *IEEE Trans. on Inform. Theory,* vol. IT-34, no. 5, pp. 1152-1187, Sept. 1988, Part II.

[2] H. C. A. van Tilborg, "The smallest length of binary 7-dimensional linear codes with prescribed minimum distance," *Discrete Mathematics,* **33** (1981), pp. 197-207.